



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,389	07/26/2001	Neil Andrew Cowie	00.177.01	5037
<div>7590 09/17/2007</div> <div>Zilka-Kotab, PC P.O. Box 721120 San Jose, CA 95172-1120</div>				
<div>EXAMINER</div> <div>HENNING, MATTHEW T</div>				
<div>ART UNIT PAPER NUMBER</div> <div>2131</div>				
<div>MAIL DATE DELIVERY MODE</div> <div>09/17/2007 PAPER</div>				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/912,389

Applicant(s)

COWIE ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) See Continuation Sheet is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) See Continuation Sheet is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Continuation of Disposition of Claims: Claims pending in the application are 1-3,5-8,12,14-19,21-24,28,30-35,37-40,44,46-51,53-56,60,62-67,69-72,76,78-83,85-88,92,94-96 and 98.

Continuation of Disposition of Claims: Claims rejected are 1-3,5-8,12,14-19,21-24,28,30-35,37-40,44,46-51,53-56,60,62-67,69-72,76,78-83,85-88,92,94-96 and 98.

1 This action is in response to the communication filed on 6/28/2007.

2 **DETAILED ACTION**

3 *Response to Arguments*

4 Applicant's arguments filed 6/28/2007 have been fully considered but they are not
5 persuasive.

6 Regarding applicants' argument that it would not have been obvious to combine the
7 teachings of Arnold in the system of Cozza because Arnold teaches detection of viruses in an
8 encrypted file, while Cozza discloses that the compressed file is decompressed prior to searching
9 for viruses, the examiner does not find the argument persuasive. First, Cozza discloses that if the
10 file requires decompression, then it is decompressed. This does not require decompression in
11 Cozza. Second, Arnold teaches an alternative to decryption when searching for viruses in an
12 encrypted file. As such, the ordinary person skilled in the art would have been motivated to
13 implement the teachings of Arnold in place of the decompression and searching of Cozza.
14 Furthermore, Cozza does not teach away from the teachings of Arnold, but rather disclosed an
15 alternative to the method of Arnold. Nowhere in Cozza is there any teaching that would cause
16 one of ordinary skill in the art to ignore or avoid the teachings of Arnold. As such, the examiner
17 does not find the argument persuasive.

18 Regarding applicants' argument that comparing the current resource fork size with
19 cached resource fork size does not meet the limitation of reading resource data within said
20 packed computer file, said resource data specifying program resource items used by said known
21 computer program, the examiner does not find the argument persuasive. First, the resource fork
22 size falls within the scope of resource data. Second, Cozza disclosed that the resource fork may

Art Unit: 2131

1 include application code, icons, preferences, strings, templates, and other such items. These all
2 fall under resource data as well. The claim does not require reading all resource data. As such,
3 by reading the resource fork size, which is part of the resource data, Cozza has met the limitation
4 of claim. Furthermore, Cozza specifically says that this may involve decompression, **or**
5 executing some other special system or other code in order to obtain this information. Therefore,
6 Cozza disclosed that decompression was not required. As such, the examiner does not find the
7 argument persuasive.

8 Regarding applicants' argument that Cozza, Arnold and Pietrek do not teach fingerprint
9 data which includes a number of program resource items specified within said resource data, the
10 examiner does not find the argument persuasive. First, RESFORKLEN is an item of resource
11 data of said packed computer file, and is part of the "fingerprint" data, and as such falls within
12 the scope of the claim language. Furthermore, the teachings of Arnold disclose generating more
13 fingerprint data by hashing the data of the file, and as such, it would have been obvious that this
14 portion of fingerprint data would include a number of resource data items from the packed
15 computer file, as required by the claim language. Therefore, the examiner does not find the
16 argument persuasive.

17 Regarding applicants' argument that the claimed fingerprint data is generated from
18 processed resource data, which is different from hashing resource data, the examiner does not
19 find the argument persuasive. Hashing is a form of processing, and therefore hashing resource
20 data is also processing resource data. The examiner further notes that the claim language does
21 not require processing "only" resource data to produce the fingerprint. As such, the examiner
22 does not find the argument persuasive.

Art Unit: 2131

1 Regarding applicants' argument that the "flags" of Cozza do not indicate which data is
2 included within said generated fingerprint data, the examiner does not find the argument
3 persuasive. First, the claim language does not require that the flag indicates all of the data that
4 was included in the generated fingerprint data. Each set of flags of Cozza indicates which
5 viruses are contained within a specific file, as can be seen in Fig. 5 and Col. 5 Paragraph 4. As
6 discussed above, the file data is used to generate the hash portion of the fingerprint. The flags
7 indicate which viruses, and thus which data, was included in the file data which is hashed, which
8 falls within the scope of the claim language. Therefore, the examiner does not find the argument
9 persuasive.

10 Regarding applicants' argument that the prior art fingerprint data does not include a
11 location within said resource data of an entry specifying a program resource item having a
12 largest size, the examiner does not find the argument persuasive. Because the file contains the
13 resource fork and resource items, and the hash is taken of the file, the signature includes a
14 number of resource items specified within the resource fork, including the location of the entries
15 of the resource items, including the largest resource item. Similarly, because the hash is of the
16 file, the hash includes all locations within the file. As such, the examiner does not find the
17 argument persuasive.

18 Regarding applicants' argument that the relied upon prior art does not teach that the
19 "checksum" is dependant upon a number of program resources...of said packed computer file,
20 the examiner does not find the argument persuasive. The applicants' seem to have
21 misinterpreted the rejection. The examiner is relying on the "hash", as taught by Arnold, in the

Art Unit: 2131

1 combination, as meeting the limitation of the checksum, and not the checksum of the cache
2 disclosed by Cozza. As such, the examiner does not find the argument persuasive.

3 Regarding applicants' argument with respect to claim 12, that the prior art relied upon
4 does not teach the fingerprint including timestamp data indicative of a time of compilation of
5 said known computer program, the examiner does not find the argument persuasive. As the hash
6 is of the file, and Win32 PE files include this timestamp, it would have been obvious that it
7 would be included in the hash (See Pietrek Page 6 TimeDateStamp). As such, the examiner does
8 not find the argument persuasive.

9 Regarding applicants' request for evidence that SHA has a "rotation" between items, the
10 examiner provides Schneier (Applied Cryptography, Second Edition) and directs the applicant to
11 pages 442-445, especially Fig. 18.7 which shows the "rotation" in SHA, called a left circular
12 shift, and each block of data reads on the "item". As such, the examiner does not find the
13 argument persuasive.

14 Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72,
15 76, 78-83, 85-88, 92, 94-96, and 98 have been examined, while claims 4, 9-11, 13, 20, 25-27, 29,
16 36, 41-43, 45, 52, 57-59, 61, 68, 73-75, 77, 84, 89-91, 93, and 97 have been cancelled.

17 All objections and rejections not set forth below have been withdrawn.

18
19 ***Claim Rejections - 35 USC § 103***

20 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
21 obviousness rejections set forth in this Office action:

22 *A patent may not be obtained though the invention is not identically disclosed or*
23 *described as set forth in section 102 of this title, if the differences between the subject matter*

Art Unit: 2131

1 *sought to be patented and the prior art are such that the subject matter as a whole would have*
2 *been obvious at the time the invention was made to a person having ordinary skill in the art to*
3 *which said subject matter pertains. Patentability shall not be negated by the manner in which*
4 *the invention was made.*
5

6 Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72,
7 76, 78-83, 85-88, 92, 94-96, and 98 are rejected under 35 U.S.C. 103(a) as being unpatentable
8 over Cozza (US Patent Number 5,649,095), and further in view of Arnold et al. (US Patent
9 Number 5,442,699), hereinafter referred to as Arnold, and further in view of Pietrek ("Peering
10 Inside the PE: A Tour of the Win 32 Portable Executable").

11 Regarding claims 1, 17, 33, 49, 65, and 81, Cozza disclosed a system, method, and
12 computer program product in a computer storage medium (See Cozza Claims and Col. 1 Lines
13 26-33) comprising a computer program operable to control a computer to detect a known
14 computer program within a packed computer file, said packed computer file being unpacked
15 upon execution, said computer program comprising (See Cozza Abstract and Col. 3 Paragraph
16 6): resource data reading logic for reading resource data within said packed computer file (See
17 Cozza Col. 6 Lines 21-23 and 29-34), said resource data specifying program resource items used
18 by said known computer program (See Cozza Col. 2 Paragraph 7) and readable by a computer
19 operating system without dependence upon which unpacking algorithm is used by said packed
20 computer file (See Cozza Col. 6 Paragraphs 2-3 wherein the compressed file is not decompressed
21 in order to read the resource forks information); and resource data comparing logic for
22 generating characteristics of said resource data (See Cozza Col. 1 Lines 58-65 wherein it was
23 inherent that the characteristic data was generated in order for the data to have been compared)
24 and for comparing said characteristics of said resource data with characteristics of resource data

1 of said known computer program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-65) and for
2 detecting a match with said known computer program indicative of said packed computer file
3 containing said known computer program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-
4 65), wherein said resource data of said packed computer file is processed to generate fingerprint
5 data (See Cozza Fig. 5); wherein said generated fingerprint data includes a number of program
6 resource items specified within said resource data of said packed computer file (See Cozza Fig. 5
7 RESFORKLEN); wherein said generated fingerprint data includes a flag indicating which data is
8 included within said generated fingerprint data (See Cozza Fig. 5); wherein said generated
9 fingerprint data includes a checksum value of the computer file (See Cozza Fig. 5), but Cozza
10 failed to specifically disclose wherein said generated fingerprint data is compared with
11 fingerprint data of said known computer program; wherein the fingerprint data included a
12 location within said resource data of an entry specifying a program resource item having a
13 largest size (See Cozza Col. 6 Lines 29-45); or that the checksum value was calculated in
14 dependence upon: a number of said program resource items specified beneath each node within
15 hierarchically arranged resource data of said packed computer file; string names associated with
16 said program resource items within said resource data of said packed computer file; and sizes of
17 said program resource items within said resource data of said packed computer file. However,
18 Cozza did disclose the file including a number of program resource items specified within said
19 resource data (See Cozza Col. 2 Paragraph 7).

20 Pietrek teaches that a Win32 PE file is an executable file which contains un-initialized
21 code and resources, which when executed the code is initialized using the resources (See Pietrek
22 Page 21 PE File Base Relocations).

1 Arnold teaches a method of virus scanning in which hashes of a file are created and
2 compared to hashes of known viral patterns in order to detect computer viruses upon matching
3 (See Arnold Col. 10 Lines 48-52).

4 It would have been obvious to the ordinary person skilled in the art at the time of
5 invention to employ the teachings of Pietrek in the virus detector of Cozza by allowing the
6 scanning of Win32 PE files and their resources. This would have been obvious because the
7 ordinary person skilled in the art would have been motivated to provide protection against Win32
8 PE files containing viruses.

9 It further would have been obvious to the ordinary person skilled in the art at the time of
10 invention to employ the teachings of Arnold in the virus scanning of Cozza by creating hashes of
11 the data, including the resources, of the compressed file and comparing it to hashes of known
12 viral patterns. This would have been obvious because the ordinary person skilled in the art
13 would have been motivated to scan the files as quickly as possible, without compromising
14 security.

15 It would have been obvious in this combination that because the file contains the resource
16 fork and resource items, and the hash is taken of the file, the signature includes a number of
17 resource items specified within the resource fork, including the location of the entries of the
18 resource items, including the largest resource item. It further would have been obvious that
19 because the fingerprint data represented the file during comparison, and the flags of Cozza
20 indicated the viruses found in the file, the fingerprint data would have included a flag indicating
21 which data (viruses) was included within said fingerprint data.

1 It further would have been obvious that the checksum (hash) of the file in this
2 combination would have been dependant upon a number of said program resource items
3 specified beneath each node within hierarchically arranged resource data of said packed
4 computer file; string names associated with said program resource items within said resource
5 data of said packed computer file; and sizes of said program resource items within said resource
6 data of said packed computer file, as Pietrek teaches that Win32 PE files are arranged in such a
7 manner, as is seen in Pietrek Fig. 5 and Table 13.

8 Regarding claims 2, 18, 34, 50, 66, and 82, Cozza, Arnold, and Pietrek disclosed that said
9 known computer program is one of: a Trojan computer program; and a worm computer program
10 (See Cozza Col. 1 Lines 22-32 and Col. 7 Lines 35-39).

11 Regarding claims 3, 19, 35, 51, 67, and 83, Cozza, Arnold, and Pietrek disclosed that said
12 resource data comparing logic is operable to compare said resource data with characteristics of a
13 plurality of known computer programs to detect if said packed computer program contains one of
14 said plurality of known computer programs (See Cozza Col. 7 Lines 35-40).

15 Regarding claims 5, 21, 37, 53, 69, and 85, Cozza, Arnold, and Pietrek disclosed that said
16 program resource items used by said known computer program include one or more of: icon
17 data; string data; dialog data; bitmap data; menu data; and language data (See Cozza Col. 2
18 Paragraph 7).

19 Regarding claims 6-8, 22-24, 38-40, 54-56, 70-72, and 86-88, the combination of Cozza,
20 Arnold, and Pietrek disclosed specifying a storage location for each resource item as an offset,
21 and the size of each resource (See Pietrek Page 20 Table 13 Offsets and Page 21 Fig. 14
22 DWORD OffsetToData).

9 Regarding claims 15, 31, 47, 63, 79, and 95, Cozza, Arnold, and Pietrek disclosed
0 decompressing the computer program upon execution (See Pietrek Page 21 PE File Base
1 Relocations).

3

4

5 Conclusion

6 Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72,
7 76, 78-83, 85-88, 92, 94-96, and 98 have been rejected.

8 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time
9 policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after


Art Unit: 2131

1 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period
2 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
3 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
4 however, will the statutory period for reply expire later than SIX MONTHS from the mailing
5 date of this final action.

6 Any inquiry concerning this communication or earlier communications from the
7 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
8 The examiner can normally be reached on M-F 8-4.

9 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
10 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
11 organization where this application or proceeding is assigned is 571-273-8300.

12 Information regarding the status of an application may be obtained from the Patent
13 Application Information Retrieval (PAIR) system. Status information for published applications
14 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
15 applications is available through Private PAIR only. For more information about the PAIR
16 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
17 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

18
19
20
21
22
23
24 
25 Matthew Henning
26 Assistant Examiner
27 Art Unit 2131
9/11/2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100